

EZJ KDV B

21 MAG 3891UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States Of America for a Search and Seizure Warrant for the forensic image of an Apple iPhone with IMEI No. 353897100042680, and IMSI No. 310260240063546, USAO No. 2021R00338

**Agent Affidavit in Support of
Application for Search and Seizure
Warrant**

SOUTHERN DISTRICT OF NEW YORK) ss.:

WILLIAM CLARK, being duly sworn, deposes and says:

I. Introduction**A. Affiant**

1. I have been a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations (“HSI”) for approximately four years. I am currently a member of the Violent Gang Task Force. Prior to joining HSI, I was a Special Agent with the Internal Revenue Service - Criminal Investigation for approximately five years. I have investigated narcotics, racketeering, and firearms offenses similar in nature to the suspected offenses outlined below, and have participated in the execution of search warrants for electronic evidence of the sort requested here. Through my training, education and experience, I have become familiar with the manner in which extortion schemes are operated.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic device specified below (the “Subject Device”) for the items and information described in Attachment A, which is incorporated by reference. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the

forensic analysis of electronically stored information (“ESI”). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Device

3. The Subject Device is particularly described as the forensic image of an Apple iPhone with IMEI No. 353897100042680 and with IMSI No. 310260240063546.

4. Based on my training, experience, and research, I know that the Apple iPhone with IMEI No. 353897100042680 and with IMSI No. 310260240063546, from which the forensic image was created, has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, address book, calendar, and GPS navigation device.

5. The Subject Device is presently located in HSI custody in the Southern District of New York.

C. The Subject Offenses

6. For the reasons detailed below, I believe that there is probable cause to believe that the Subject Device contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1951 (Hobbs Act extortion); 1959 (violent crimes in aid of racketeering); and 1962(d) (racketeering conspiracy) (the “Subject Offenses”).

II. Probable Cause

A. Probable Cause Regarding Commission of the Subject Offenses

7. HSI and the Federal Bureau of Investigation (“FBI”) have been investigating a fire mitigation company based in Brooklyn, New York named First Response Cleaning Corp. (“First Response”). The investigation has shown that members of the Bloods gang, including Target

Subject Jatiel SMITH, a/k/a “Tiek,” have taken control of First Response and are using First Response to make money for the gang through extortion, fraud, and assault.

8. Based on my participation in this investigation, including my discussions with other members of law enforcement, I know that when properties suffer fire damage, the property owners sometimes hire a public adjuster to investigate and process the insurance claim. The public adjuster, in turn, hires an emergency mitigation service, or “EMS,” to clean up the damaged property, which often includes sweeping up and removing debris, airing out the property, and boarding up the property. First Response is an EMS. As set forth below, it appears that employees of First Response have been threatening public adjusters with violent force unless the public adjusters hire First Response as their EMS.

9. Based on an interview law enforcement conducted with an insurance adjuster based in New York who has worked with First Response in the past (“Witness-1”), I know the following:

- a. In approximately early 2020, reports of violence by First Response employees began circulating in the insurance industry. For example, there was a report that the owner of First Response’s competitor EMS company was beat up and the company went out of business. In another incident, a public adjuster’s office was attacked with bricks.
- b. According to Witness-1, the public adjusters can no longer hire an EMS other than First Response unless the insured calls directly. First Response has also blocked other EMS companies from responding to fires at night. Witness-1 stated that where there used to be eight or nine EMS companies on the scene of a fire, now there is sometimes just First Response.
- c. Witness-1 heard that First Response was using members of the Bloods gang to collect money.

10. Based on an interview law enforcement conducted with a public adjuster based in Queens, New York (“Victim-1”), I know the following:

- a. In or about December 2019, Victim-1 heard that employees of First Response were intimidating competitors, including the owner of a competing EMS who was assaulted and put into a coma. At about the same time, Victim-1 spoke to Carl Walsh, the nominal owner of First Response, who appeared nervous and who told Victim-1 that a First Response employee named “Teak” now makes the decisions for the company, not Walsh.
- b. Victim-1 has had approximately three interactions with the person he knows as “Teak.” Victim-1’s description of “Teak” is consistent with the physical appearance of Jatiel SMITH, a/k/a “Tiek.” During one of Victim-1’s interactions with “Teak,” “Teak” told Victim-1 that he “knocked out” the other EMS company.
- c. In approximately 2020, Victim-1 responded to a house fire. When Victim-1 arrived at the house, Victim-1 was approached by an employee of First Response, who asked Victim-1 to hire First Response as the EMS. The First Response employee then told Victim-1 that “Teak” would like a word, and handed Victim-1 a cellphone; Victim-1 spoke briefly to the person he knew as “Teak.” Victim-1 then entered the house and photographed the damage. Upon exiting the house, Victim-1 noticed that the First Response employee was still present. While Victim-1 was having the homeowner sign a retainer for the job, Victim-1 was punched in the head and fell to the ground, hitting a cement pillar.

- d. Victim-1 has also heard about other incidents in which members of First Response assaulted a public adjuster, including an assault against an employee of the public adjuster that Victim-2 (discussed below) worked for.
- e. Victim-1 stated that First Response has attempted to establish “rules” in the industry, including the rule that any fire that happens between 8pm and 8am belongs to First Response, and that the first ten fires of every month belong to First Response.

11. Based on an interview law enforcement conduct with a public adjuster based in Long Island, New York (“Victim-2”), I know the following:

- a. On or about September 15, 2020, Victim-2 had responded to a call of a house fire in Queens.
- b. Victim-2 was attacked at the scene. Victim-2 sustained a lip laceration, lost a tooth, and brain bleeding. The injuries required Victim-2 to stay overnight in the hospital.

12. Based on my review of records maintained by the New York City Department of Corrections, I know that on or about April 3, 2019, Jatiel SMITH, a/k/a “Tiek,” was arrested and housed at Riker’s Island. Records indicate that SMITH self-identified as a member of the Bloods gang.

13. I have reviewed the public postings of a Facebook account that appears to belong to Jatiel SMITH, a/k/a “Tiek” (the “Smith Facebook Account”). Among other things, the name of the account is “Tieksopetty Smith,” the account includes multiple photographs of SMITH consistent with SMITH being the user of the account, and the account has posted legal records with SMITH’s name on them, including parole discharge papers. The Smith Facebook Account includes multiple posts in which SMITH appears to discuss gang business and his affiliation with

the Bloods, and also includes posts about First Response. For example, in a July 16, 2017 post, SMITH listed the dates of his membership in various Bloods sets (“GKB 1997, KSB 2004, TSG 2007”). The Smith Facebook Account also includes multiple posts of SMITH wearing red clothing associated with the Bloods and using language associated with the Bloods. The Smith Facebook Account also includes photographs of SMITH wearing First Response gear. In a post from approximately April 2021, the Smith Facebook Account posted a photograph of a man wearing First Response gear and the message, “Last week i secured a 3.4 million job and thought it was a highlight!!! Then i woke up in go mode and secured a \$24 million dollar job!!! Oh it's definitely play time!!!!”

14. On or about March 2, 2021, at approximately 7:00 a.m., HSI was notified that SMITH was boarding a plane going from Newark International Airport to Jamaica. A few hours later, HSI was informed that SMITH was returning from Jamaica that same day and would be landing at Newark International Airport at approximately 5:00 p.m. At approximately 5:00 p.m., officers with Customs and Border Protection located and detained SMITH at Newark International Airport. The officers searched SMITH’s bags and located just under \$10,000 in cash. SMITH also had an Apple iPhone with IMEI No. 353897100042680 and with IMSI No. 310260240063546. Special Agents with HSI seized SMITH’s phone pursuant to HSI’s border search authority and requested SMITH’s passcode, which SMITH eventually provided. HSI then extracted a forensic copy of the phone contents, which forensic copy is the Subject Device. The phone was returned to SMITH.

15. Special Agents with HSI performed an initial and preliminary review of the Subject Device. The preliminary review of the Subject Device showed, revealed, among other things, that the Subject Device contained what appear to be communications in which the user of the phone

identifies himself as a member of the Bloods and discusses Bloods gang activity. The Subject Device also contained what appeared to be discussions of SMITH's work with First Response, including communications in which he discusses his remuneration arrangement and the "rules" about responding to fires, as well as communications with what appeared to be either insureds or public adjusters about submitting fraudulent insurance claims.

B. Probable Cause Justifying Search of the Subject Device

16. Based on my training and experience, as well as my participation in this investigation and other investigations, I have learned the following, in substance and in part:

a. Like individuals engaged in any other kind of activity, individuals who engage in gang activity and extortion often store records relating to their illegal activity and to persons involved with them in that activity on electronic devices such as the device that the Subject Device was copied from. Such records can include, for example, logs of online chats with co-conspirators; email correspondence; and contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts. Individuals engaged in criminal activity often store such records in order to, among other things, (1) keep track of co-conspirator's contact information; (2) keep a record of illegal transactions for future reference; and (3) keep an accounting of illegal proceeds for purposes of, among other things, dividing those proceeds with co-conspirators. Here, I believe the facts set forth above, based on my training and experience, indicate that SMITH and his co-conspirators use cellphones in connection with their extortion activity with First Response.

17. Computer files or remnants of such files can be recovered months or even years after they have been created or saved on electronic devices such as the Subject Device. Even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. Thus, the ability to retrieve

from information from the Subject Device depends less on when the information was first created or saved than on a particular user's device configuration, storage capacity, and computer habits.

III. Procedures for Searching ESI

A. Review of ESI

18. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained on the Subject Device for information responsive to the warrant.

19. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

20. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the

circumstances, however, law enforcement may need to conduct a complete review of all the ESI from the Subject Device to locate all data responsive to the warrant.

B. Return of the Subject Device

21. If the Government determines that the Subject Device is no longer necessary to retrieve and preserve the data on the device, and that the Subject Devices are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return the Subject Device, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

IV. Conclusion and Ancillary Provisions

22. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

/s/ William Clark, by SDA with permission

William Clark
Special Agent
Homeland Security Investigations

Sworn to me through the transmission of
this Affidavit by reliable electronic means,
Pursuant to Federal Rules of Criminal
Procedure 41(d)(3) and 4.1, this 9th day of
April, 2021

Stewart D. Aaron

HON. STEWART D. AARON
UNITED STATES MAGISTRATE JUDGE

Attachment A

I. Device Subject to Search and Seizure

The device that is the subject of this search and seizure warrant (the “Subject Device”) is described as follows:

The forensic image of an Apple iPhone with IMEI No. 353897100042680 and with IMSI No. 310260240063546

II. Review of ESI on the Subject Device

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Device for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1951 (Hobbs Act extortion); 1959 (violent crimes in aid of racketeering); and 1962(d) (racketeering conspiracy) (the “Subject Offenses”) described as follows:

1. Evidence concerning the identity or location of the owner(s) or user(s) of the Subject Device;
2. Evidence concerning the identity or location of, and communications with, co-conspirators;
3. Contact information, including names, phone numbers, and addresses, for any co-conspirators or other entities related to the Subject Offenses;
4. Incoming and outgoing calls related to the Subject Offenses;
5. Opened and unopened voicemail messages related to the Subject Offenses;
6. Text, data, chat, digital photographs and video, MMS (i.e., multimedia messaging service), and SMS (i.e., short message service), email messages, or messages on social media or messaging applications installed on the device (collectively, “text messages”), any attachments to those text messages, such as digital photographs and videos, and any associated information, such as the phone number or user ID from which the text message was sent, pertaining to the Subject Offenses;
7. Calendar or other scheduling information related to the Subject Offenses (including but not limited to itineraries and meetings with co-conspirators or other entities related to the Subject Offenses);
8. Historical location data showing the user’s movements;

9. Photographs related to the Subject Offenses;
10. Records pertaining to locations as well as travel (including vehicle rental records) to and from locations relating to co-conspirators or other entities related to the Subject Offenses;
11. Bank records, electronic bank statements, bank checks, credit card records, ATM card records, cash receipts, credit histories, tax records, money transfer records and receipts, money remittance instructions, customer information and records, sales records, ledgers showing cash and checks received, contracts, fax records, correspondence, checks, credit card bills, account information, and other financial records including any/all records of disputed and/or reported fraudulent charges or deposits or efforts to obtain reimbursement for alleged false or fraudulent charges or deposits relating to the Subject Offenses;
12. Evidence regarding the wiring, laundering, or withdrawal of illicitly obtained funds in furtherance of the Subject Offenses;
13. Evidence consisting of, referring to, or reflecting membership or participating in efforts to commit the Subject Offenses; and
14. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer and/or mobile devices, storage media, and related electronic equipment.